Achieving Zero-Error Capacity 1 for a Collision Channel Without Feedback

Yijin Zhang, Yi Chen, Yuan-Hsun Lo and Wing Shing Wong

Abstract

The collision channel without feedback (CCw/oFB) model introduced by Massey and Mathys, depicts a scenario in which M users share a thermal noise-free communication channel with random relative time offsets among their clocks. This paper considers an extension of this model, which allows the receiver to use successive interference cancellation (SIC) to iteratively cancel the interference caused by those collided packets that have been decoded by the receiver. As the main result of this paper, we derive the zero-error capacity region of this channel in the slot-synchronous case, and present a zero-error capacity achieving scheme by joint protocol sequences and channel coding design. It is shown that the negative impact on the zero-error capacity due to a lack of time synchronization can be removed by the help of SIC. Moreover, we characterize the protocol sequences that can be used to achieve zero-error capacity 1 [packets/slot] by proving new results on shift-invariant sequences and throughput-invariant sequences; these sequences have been known to achieve zero-error capacity for the basic CCw/oFB model without SIC. This characterization sheds light on the minimum sequence period required in order to attain zero-error capacity 1.

Index Terms

Collision channel without feedback, zero-error capacity, successive interference cancellation, protocol sequences

This work was supported by the National Natural Science Foundation of China (No. 61301107 and 11601454), and the Natural Science Foundation of Fujian Province of China (No. 2016J05021).

Y. Zhang is with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China. E-mail: yijin.zhang@gmail.com.

Y.-H. Lo is with the School of Mathematical Sciences, Xiamen University, Xiamen, China. E-mail: yhlo0830@gmail.com.

Y. Chen and W. S. Wong are with the Department of Information Engineering, The Chinese University of Hong Kong, Shatin, N. T., Hong Kong. E-mail: chelseachenyi@gmail.com; wswong@ie.cuhk.edu.hk.

I. Introduction

Consider a multiple access communication channel that is shared by M users, each one of them always has a fixed-length source packet awaiting transmission. Obviously, time-division multiple-access (TDMA) can be employed to achieve zero-error capacity 1 [packets/slot] (that is, the maximum sum rate of a point in the zero-error capacity region is one). However, it is impractical to implement such a scheme due to difficulty in ensuring stringent time synchronization among users. User mobility or propagation delays are additional exacerbating factors making this issue even more challenging. Lack of synchroneity among users invariably will lead to random pattern of channel usage with some slots completely devoid of any transmissions, while others may contain garbled signals due to contention. Under the classic collision channel model, such channel usage patterns will cause loss of channel capacity.

To determine how much loss of transmission capacity occurs when users are prevented from time-sharing, Massey and Mathys introduced a model of *collision channel without feedback* (CCw/oFB) [1], and investigated its zero-error capacity region. The central idea of this seminal work is to employ erasure correcting coding across source packets to recover data loss due to collisions and to use *protocol sequences*, which are deterministic $(0, 1)$-binary sequences with special Hamming cross-correlation properties, to specify when the users transmit. By application of these two techniques, is was shown in [1] that the symmetric zero-error capacity of the CCw/oFB model (that is, the maximum sum rate of a point in the zero-error capacity region where all users have identical information rates) is $(1 - \frac{1}{M})^{M-1}$ [packets/slot]. Hence, in comparison with a TDMA system, the lack of a common time reference yields a substantial amount of capacity loss.

A wireless system can handle unavoidable collisions by treating them simply as erasures, or by applying *successive interference cancellation* (SIC) techniques as in [2]–[6]. At the signal processing level, SIC is employed to iteratively cancel the interference caused by collided packets which have been decoded by the receiver in previous iterations. By providing a chance for all collided packets to be correctly received, this strategem significantly improves the transmission capacity of a random access scheme, and offers a possibility to fully utilize a collision channel.

To exploit SIC in a random access channel, the scheme in [2] encodes source packets by erasure correcting codes prior to transmission, while in [3]–[6] user packets are simply repeated for

channel coding. The established connection between SIC and erasure correcting coding motivates us to investigate how to design protocol sequences and coding schemes under the SIC framework in order to improve the zero-error capacity of a CCw/oFB model.

The main result of this paper is that the zero-error capacity of a CCw/oFB model with SIC has a maximum sum rate equal to 1[packets/slot] for any number of users. Moreover, any rate vector with rational number components that satisfies this maximum sum rate condition is achievable, as in a TDMA system. This implies an interesting corollary that the negative impact on the zero-error capacity due to a lack of a common time reference can be removed by the employment of SIC at the signal processing level.

Our second result is that the protocol sequences that can be used to achieve zero-error capacity 1 in a CCw/oFB model with SIC can be uniquely characterized via shift-invariant sequences [1], [7]. In the design of protocol sequences, a common objective is to aim for sequences with short periods, since it is clear that short sequence period implies short channel access delay. In [7], explicit algorithms for constructing shift-invariant sequences with shortest common periods are presented. These uniquely characterized solutions provide a method for achieving zero-error capacity. They also help us understand how short the sequence period can be for achieving zero-error capacity 1.

In [2], results on a slotted ALOHA model with SIC were presented under the context of a collision channel without feedback. However, [2] and related papers [3]–[5] all assumed that each user has a fixed probability to access the channel in each time slot and time synchronization is needed at the beginning of each MAC frame. One exception is [6], which assumed Poisson arrival packets for each user and did not require frame synchronization. Although the system model considered in [2]–[6] may be more practical in some applications with a large and time varying population of active users, the CCw/oFB model in [1] that we follow here is more appropriate for evaluating the capacity loss due to a lack of time synchronization. Moreover, the schemes described in [2]–[6] only apply to the symmetric case and it is difficult to determine the zero-error capacity due to their probabilistic nature.

The organization of the rest of this paper is as follows. In Section II, we present a model of CCw/oFB with SIC, as an extension of the basic CCw/oFB model. Some useful concepts and background results of protocol sequences are introduced in Section III. In Section IV, we provide the main results of this paper, which include the key result on zero-error capacity region and

the uniquely characterized protocol sequences for achieving zero-error capacity 1. In Section V, a proof of results in Section IV is presented. We offer some concluding remarks in Section VI.

II. Channel Model

Now we first introduce the basic model of CCw/oFB [1], and then present an extended model with SIC.

A. The Basic CCw/oFB Model

Consider a noiseless communication channel without feedback that is shared by M users. Each user has an independent and memoryless *Q-ary symmetric source* (QSS) ($Q \geq 2$), which produces a nonempty queue of fixed-length source *packets* (or interchangeably referred to as *symbols*) to be transmitted to a common receiver.

As no channel state feedback is available, in order to provide reliable communication without relying on retransmissions, user i, for $i = 1, 2, \ldots, M$, employs an (n_i, m_i) erasure correcting coding to encode a block of m_i source packets to a block of n_i ($n_i \geq m_i \geq 1$) coded packets for actual transmission on the channel, such that the m_i source packets can be decoded if any m_i of the n_i coded packets can be received correctly. It is not required that coding must be used prior to transmission for each user, that is, it is possible that $n_i = m_i = 1$ for some i. However, all transmitted packets on the channel are viewed as coded packets. For the sake of completeness, we define a user who always keeps silent in a communication session to be employing a $(0, 0)$ erasure correcting coding. We assume that (n_i, m_i) is fixed for each user i during every communication session.

For simplicity reasons, we ignore propagation delays here. Due to the lack of feedback, a common time reference between any of the users or the receiver is unavailable, and hence, there are *relative time offsets*. Offset δ_i of user i, for $i = 1, 2, \ldots, M$, is defined such that a signal from user i, received at time t on the receiver's clock, was actually sent at time $t - \delta_i$ on user i's clock. These relative time offsets are random, always unknown to the users, but unchanged in a communication session. In this paper, we restrict our attention to the *slot-synchronous* case, that is, the time offsets $\delta_1, \delta_2, \ldots, \delta_M$ are arbitrary integer multiples of T. We define a time slot to be a semi-open interval with time length T.

Following [1], for every i, user i's transmission schedule on a CCw/oFB for coded packets can be described by its *protocol signal* $x_i(t)$, which has $(0,1)$ binary value for all t, and takes on the value one only over semi-open intervals whose lengths are integer multiples of T. If $x_i(jT)=1$, user i transmits a coded packet for one time slot duration starting on the time instant $jT+\delta_i$ at the receiver's clock. Otherwise, it keeps silent (i.e., emit the zero waveform) at that time interval. We require that $x_i(t)$ has finite period and no finite bound in time. Define the *duty factor* p_i of user i as the fraction of time of a period during which $x_i(t)=1$. Obviously, $0\leq p_i\leq 1$. Note that if user i is transmitting source packets at a positive rate R_i packets/slot, then $0<p_i\leq 1$ and the information rate inside the coded packets is R_i/p_i; if user i is transmitting source packets at a zero rate, then $p_i=0$.

A coded packet transmitted at the time interval $[t,t+T)$ is assumed to be in a collision if some other coded packet begins its transmission at t', $t-T<t'<t+T$, and it is correctly received if it does not collide with other users. In the basic CCw/oFB model, coded packets involved in collisions are all considered to be totally lost.

As proposed by Massey and Mathys in [1], if users always transmit or keep silent for semi-open intervals whose lengths are integer multiples of one time slot, we can equivalently describe the protocol signal $x_i(t)$ by a binary *protocol sequence* $\mathrm{s}_i:=[s_i(0)\ s_i(1)\ \ldots\ s_i(L-1)]$, for $i=1,2,\ldots,M$, where L is the common sequence period of all M sequences. Define $\tau_i:=\delta_i/T$ to be the *relative shift* of user i in relation to the receiver in units of one time slot duration. In the slot-synchronous case, all users transmit their coded packets align to the common slot boundaries by protocol sequences. If $s_i(n \mod L)=1$, user i transmits one coded packet within the $(n+\tau_i)$-th time slot on the receiver's clock, and otherwise, keeps silent within the $(n+\tau_i)$-th time slot on the receiver's clock. The duty factor p_i is obviously the fraction of ones in s_i. Collisions occur only when coded packets completely overlap. Following [1], we also require that user i encodes one block of source packets to one block of coded packets for transmission during successive Lp_i slots in which user i actually uses the channel, when protocol sequences are used as protocol signals.

We note that Hui [8] and Thomas [9] employed error correcting coding in a slot-asynchronous CCw/oFB to recover some partially overlapped coded packets. Tinguely et al. in [10] assumed that each collided coded packet in a slot-synchronous CCw/oFB has a certain recovery probability profiting from multiuser detection, and analyzed the capacity of such a model. However, these

more general scenarios will not be considered in this paper.

B. The CCw/oFB Model with SIC

Motivated by recent work for slotted ALOHA with SIC [2]–[5], in this paper we consider an extension of the basic CCw/oFB model that employs SIC techniques to iteratively cancel interferences caused by colliding packets.

Following [2]–[5], we assume an ideal SIC process in our channel model, which relies on ideal channel parameter estimation. This assumption simplifies the analysis of the impact of SIC on the basic model, and also suits our purposes for determining the zero-error capacity of a scheme and finding capacity achieving schemes.

Given an (n_i, m_i) coding scheme for user i, an ideal SIC should possess the following two properties: (i) Whenever any m_i of a block of n_i coded packets from user i for some i are correctly received, the receiver is capable to decode these n_i coded packets and further remove the contribution of them from the signal received in the corresponding time intervals. (ii) A coded packet can be received correctly if it does not experience a collision or signals from coded packets that overlap with it have all been subtracted. The SIC proceeds iteratively until no coded packets can be correctly received.

To ensure ideal SIC operation in our model, we assume that the receiver knows the coding schemes adopted by the users in advance, for the purpose of decoding coded packets in collisions. Obviously, it is also required that the receiver needs to identify the sender of each correctly received coded packet, and can find the location of each collided packet that the receiver want to apply the interference cancellation process. In [2]–[5], these two tasks are addressed by additional header information. Nevertheless, in Section V, we will show that the receiver can solve them by merely observing the channel outputs, following some previously known results in [1] and [7].

One example of an SIC procedure for three users is illustrated in Fig. 1. Suppose $m_1 = n_1 = 1$, $m_2 = m_3 = 1$, $n_2 = n_3 = 2$. Then the receiver can correctly receive all coded packets transmitted on the channel, and decode source packets from each user. Note that user 1 does not carry out a coding of its source packet in the shown example.

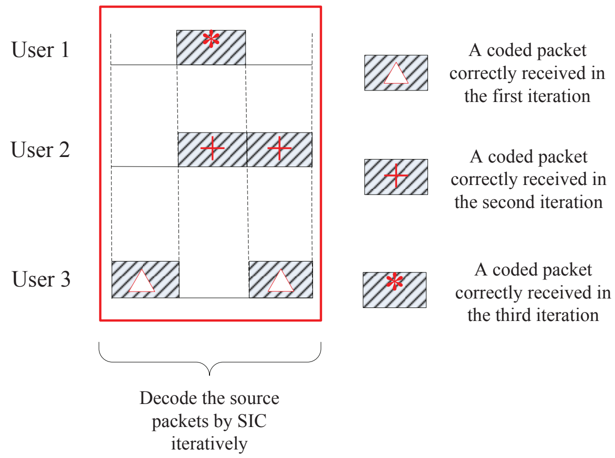

Fig. 1. An SIC procedure for three users.

III. Preliminaries on Protocol Sequences

We present some basic concepts and previously known results on protocol sequences in this section to facilitate our subsequent discussion.

Define the *Hamming weight* of $\mathbf{s}_i$, denoted by w_i, as the number of ones in a period of $\mathbf{s}_i$.

The *cyclic shift* of $\mathbf{s}_i$ by τ_i is defined as

$$\mathbf{s}_i^{(\tau_i)} := [s_i(-\tau_i)\ s_i(1-\tau_i)\ \ \ldots\ \ s_i(L-1-\tau_i)],$$

where the substraction is taken modulo L.

We identify the M users by means of the index set $\mathcal{M} := \{1, 2, \ldots, M\}$.

For $\mathcal{A} = \{i_1, i_2, \ldots, i_{|\mathcal{A}|}\}$ in $\mathcal{M}$, let $\boldsymbol{\tau}_\mathcal{A} = (\tau_{i_1}, \ldots, \tau_{i_{|\mathcal{A}|}})$, and $\mathbf{b}_\mathcal{A} = (b_{i_1}, \ldots, b_{i_{|\mathcal{A}|}})$, in which $b_{i_j} \in \{0, 1\}$ for $1 \leq j \leq |\mathcal{A}|$. The $|\mathcal{A}|$-*wise generalized Hamming cross-correlation* function associated with $\mathcal{A}$ and $\mathbf{b}_\mathcal{A}$ is defined as the number of slot indices n, $0 \leq n < L$, such that $s_{i_j}(n - \tau_{i_j}) = b_{i_j}$ for $1 \leq j \leq |\mathcal{A}|$, i.e.,

$$H\Big(\mathbf{b}_\mathcal{A}; \boldsymbol{\tau}_\mathcal{A}; \mathcal{A}\Big) := \sum_{n=0}^{L-1} \prod_{j=1}^{|\mathcal{A}|} \delta_{s_{i_j}(n-\tau_{i_j}) b_{i_j}}. \tag{1}$$

In the above equation, $\delta_{s_{i_j}(t-\tau_{i_j}) b_{i_j}}$ represents Kronecker's delta. The cross-correlation function in (1) is said to be *shift-invariant* (SI) if it is a constant function over $\boldsymbol{\tau}_\mathcal{A}$. In particular, any 1-wise generalized Hamming cross-correlation is only determined by the sequence period and Hamming weight, and hence must be SI.

The following is a well-known fundamental result of generalized Hamming cross-correlations, initially proved in [12] for a pair of sequences, and then generalized in [7] for multiple sequences.

Lemma 1 ([7]). *For any $\mathcal{A}$ in $\mathcal{M}$, we have:*

$$\sum_{\tau_{i_1}=0}^{L-1}\sum_{\tau_{i_2}=0}^{L-1}\cdots\sum_{\tau_{i_{|\mathcal{A}|}}=0}^{L-1} H\Big(\mathbf{b}_{\mathcal{A}};\boldsymbol{\tau}_{\mathcal{A}};\mathcal{A}\Big) = L\prod_{j=1}^{|\mathcal{A}|} H\Big(b_{i_j};\tau_{i_j};i_j\Big).$$

By the generalized Hamming cross-correlation defined in (1), we define the following two classes of protocol sequences:

(i) A sequence set is said to be SI [7] if $H(\mathbf{b}_{\mathcal{A}};\boldsymbol{\tau}_{\mathcal{A}};\mathcal{A})$ is SI for every $\mathcal{A}$ in $\mathcal{M}$ and all-one $\mathbf{b}_{\mathcal{A}}$.

(ii) A sequence set is said to be *throughput-invariant* (TI) [11] if $H(\mathbf{b}_{\mathcal{M}};\boldsymbol{\tau}_{\mathcal{M}};\mathcal{M})$ is SI for every $\mathbf{b}_{\mathcal{M}}$ with exactly one "1".

The TI property is necessary for protocol sequences that can be used to achieve the outer boundary of the zero-error capacity region of a CCw/oFB model without adopting SIC. Massey and Mathys in [1] presented a special class of TI protocol sequences, which indeed are SI sequences. Recently, it is proved in [11] that the SI property and TI property of a sequence set are actually equivalent. We note further that a lower bound on the period of SI protocol sequences is derived in [7].

Lemma 2 ([7]). *For any SI sequence set of M sequences with duty factors $r_1/d_1, r_2/d_2, \ldots, r_M/d_M$, such that $\gcd(r_i, d_i) = 1$ for all i, the sequence period is divisible by $d_1 d_2 \cdots d_M$. In particular, the sequence period is at least $d_1 d_2 \cdots d_M$.*

In addition, a general construction of minimum-period SI sequences for any duty factors with only rational components is presented in [7]. The recursive algorithm is summarized below for the convenience of the readers.

Construction [7]: Let $r_1/d_1, r_2/d_2, \ldots, r_M/d_M$ be given duty factors such that $\gcd(r_i, d_i) = 1$ for all i. For $i = 1, 2, \ldots, M$, we construct $\mathbb{G}_i = [\mathbf{G}_{i,1}, \mathbf{G}_{i,2}, \ldots, \mathbf{G}_{i,d_i}]$, a $\left(\prod_{j=1}^{i-1} d_j\right) \times d_i$ array of zeros and ones such that there are exactly r_i ones in each row. ($\prod_{j=1}^{0} d_j$ is defined as 1, as the empty product is equal to 1 by convention.) Note that $\mathbf{G}_{i,k}$ is the k-th column vector of $\mathbb{G}_i$ for $k = 1, 2, \ldots, d_i$. Then construct sequence $\mathbf{s}_i$ of sequence period $\prod_{j=1}^{M} d_j$, by repeating the

row vector $[\mathbf{G}_{i,1}^T\mathbf{G}_{i,2}^T\dots\mathbf{G}_{i,d_i}^T]$ for $\frac{\prod_{j=1}^M d_j}{\prod_{j=1}^i d_j}$ times, that is

$$\mathbf{s}_i = \underbrace{[\mathbf{G}_{i,1}^T\mathbf{G}_{i,2}^T\dots\mathbf{G}_{i,d_i}^T, \mathbf{G}_{i,1}^T\mathbf{G}_{i,2}^T\dots\mathbf{G}_{i,d_i}^T, \cdots, \mathbf{G}_{i,1}^T\mathbf{G}_{i,2}^T\dots\mathbf{G}_{i,d_i}^T]}_{\prod_{j=1}^M d_j \text{ sequence entries}}.$$

In this paper, we show that SI sequences maintain their essential role in achieving zero-error capacity 1 for a CCw/oFB model with SIC.

IV. Main Results

For the slot-synchronous case, the zero-error capacity region of a basic CCw/oFB model (SIC not adopted) has been derived in [1]. The outer boundary of the region is shown to be the set of all points $(C_1, C_2, \dots, C_M)$, such that

$$C_i = p_i \sum_{i=1, i\neq j}^{M} (1 - p_j), \tag{2}$$

where $(p_1, p_2, \dots, p_M)$ is a probability vector with $p_i \geq 0$ for all i and $\sum_{i=1}^M p_i = 1$.

Following [1], we define the *zero-error capacity region* $\mathcal{C}_{s0}$ of an M-user slot-synchronous CCw/oFB model operating under SIC as the set of all information rate vectors $(R_1, R_2, \dots, R_M)$, with $R_i \geq 0$ for $i = 1, 2, \dots, M$, that are *approachable*. By approachable, we require that for any i and any arbitrarily small positive η, there exist a protocol signal, $x_i(t)$, with duty factor p_i, a block code of length n_i packets for each user i such that:

(i) blocks of at least $\lceil n_i(R_i/p_i - \eta)\rceil$ source packets from the QSS for user i are encoded into blocks of n_i coded packets for transmission during successive slots in which user i actually uses the channel; and

(ii) a decoder with SIC can, from the channel output signal, reconstruct the output sequence of user i's QSS without error, regardless of the relative time offsets.

A rate vector in a capacity region is said to be *achievable* if this rate vector satisfies the above definition of an approachable rate with η set to 0.

Our first main result for $\mathcal{C}_{s0}$, is as follows.

Theorem 3. *For an M-user slot-synchronous CCw/oFB model with SIC, the outer boundary of $\mathcal{C}_{s0}$ is the set of all points $(C_1, C_2, \dots, C_M)$, such that $\sum_{i=1}^M C_i = 1$.*

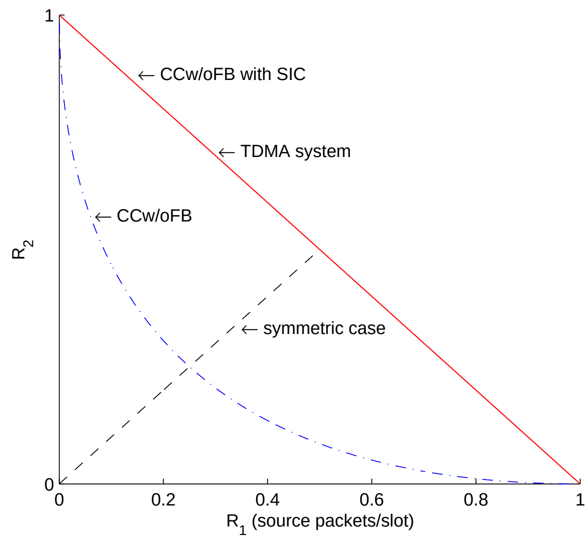

Fig. 2. Zero-error capacity region of two-user slot-synchronous CCw/oFB model with SIC compared with other systems.

Theorem 3 shows that the zero-error capacity of a CCw/oFB model is significantly improved by the help of SIC, but cannot exceed the limit of a typical collision channel: 1 [packets/slot]. Theorem 3 further implies the following two interesting consequences:

(i) The zero-error capacity region of a CCw/oFB model with SIC coincides with that of a collision channel with a common time reference, i.e., a TDMA system. In other words, the negative impact of a lack of a common time reference on the capacity can be completely removed by the employment of SIC.

(ii) The symmetric case in which all users transmit packets at the same rate $1/M$ is on the outer boundary of the capacity region. This is different from the result for random-access systems stated in [1]. For such models, the symmetric case minimizes the function $\sum_{i=1}^{M} C_i$ as claimed in [1].

Fig. 2 illustrates the last remark by showing the zero-error capacity region of a two-user slot-synchronous CCw/oFB model with SIC, in comparison with a TDMA system.

Our second main result shows that a point on the outer boundary of $\mathcal{C}_{s0}$ is achievable if this point has only rational components. Moreover, SI sequence sets with selective combinations of duty factors provide the only protocol-sequences-based solutions to attain these points on the

outer boundary. As the sequence period has a fundamental impact on the channel access delays, we are interested in the minimum period of protocol sequences that can be used to achieve the outer boundary of $\mathcal{C}_{s0}$. Hence, this result further implies that we cannot find protocol sequences shorter than the minimum-period SI sequences for achieving these points. The second result is summarized by the following theorem.

Theorem 4. *For an M-user slot-synchronous CCw/oFB model with SIC, a protocol sequence set can be used to achieve a point $(R_1, R_2, \ldots, R_M)$ such that $\sum_{i=1}^{M} R_i = 1$ which has only rational components, if and only if*

(i) this sequence set has duty factors $p_{q_1} = \frac{R_{q_1}}{1-\sum_{j=2}^{M} R_{q_j}}, p_{q_2} = \frac{R_{q_2}}{1-\sum_{j=3}^{M} R_{q_j}}, \ldots, p_{q_M} = R_{q_M}$, in which $(q_1, q_2, \ldots, q_M)$ is a permutation of $(1, 2, \ldots, M)$; and

(ii) this sequence set is SI.

From Theorem 4, one sees that there are different combinations of duty factors for achieving a given rate vector on the outer boundary of $\mathcal{C}_{s0}$. It is natural to ask for the one that leads to the shortest sequence period. We can solve this by exhaustive search with the aid of Lemma 2.

One is usually most interested in the symmetric case. The following result directly follows from Theorem 4, Lemma 2 and the construction algorithm of minimum-period SI sequences.

Corollary 5. *For a protocol sequence set achieving the symmetric rate $(\frac{1}{M}, \frac{1}{M}, \ldots, \frac{1}{M})$ in an M-user slot-synchronous CCw/oFB model with SIC,*

(i) the duty factor combination $(p_1, p_2, \ldots, p_M)$ is a permutation of $(\frac{1}{M}, \frac{1}{M-1}, \ldots, 1)$; and

(ii) the minimum period is $M!$.

It was shown in [11] that the minimum period of a protocol sequence set achieving the symmetric zero-error capacity of the basic M-user slot-synchronous CCw/oFB model is M^M. Compared to M^M, $M!$ for the SIC case is significantly shorter, and hence is more favorable for implementing an ideal SIC process and for reducing the channel access delay.

In a CCw/oFB model with SIC, as the receiver cannot correctly receive multiple signals at any time instant, we know that rate vectors with $\sum_{i=1}^{M} R_i > 1$, i.e., the rate vectors outside the zero-error capacity region $\mathcal{C}_{s0}$ cannot be approached, although collisions are not simply viewed as erasures. On the other hand, Theorem 4 implies that every rate vector on the outer boundary

of $\mathcal{C}_{s0}$ is approachable, and hence all interior points of $\mathcal{C}_{s0}$ are also approachable. Therefore, Theorem 3 is an immediate consequence of Theorem 4. A proof of Theorem 4 will be given in the following section.

V. Zero-Error Capacity 1 Achieving Protocol Sequences

In this section, we will give separate proofs to the necessity and sufficiency statements of Theorem 4.

Before proving the necessity part of the theorem, we first present a lemma which plays a central role in the proof. The lemma is a generalization of the result proven in [7] that stated equivalent conditions to the SI property for protocol sequences. One can also regard it as a generalization of the statement that TI sequences must be SI proven in [11]. We relegate the proof of the lemma to the Appendix in order not to clutter the presentation.

Lemma 6. *Let $\{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_M\}$ be a set of M binary sequences of sequence period L. The following conditions are equivalent.*

(i) There exists a $\mathbf{b}^*_{\mathcal{M}}$ such that $H(\mathbf{b}^*_{\mathcal{M}}; \boldsymbol{\tau}_{\mathcal{M}}; \mathcal{M}) > 0$ for any $\boldsymbol{\tau}_{\mathcal{M}}$, and the function $H(\mathbf{b}^*_{\mathcal{M}}; \boldsymbol{\tau}_{\mathcal{M}}; \mathcal{M})$ is SI.

(ii) $H(\mathbf{b}_{\mathcal{A}}; \boldsymbol{\tau}_{\mathcal{A}}; \mathcal{A})$ is SI for any $\mathcal{A}$ in $\mathcal{M}$ and any $\mathbf{b}_{\mathcal{A}}$.

A simple observation for a set of protocol sequences achieving zero-error capacity 1 for a CCw/oFB model with SIC is that, it must contain one and only one protocol sequence with duty factor 1. This is due to the fact that, if no sequence has duty factor 1, we can always find a combination of relative shifts to generate a silent slot which implies that zero-error capacity 1 cannot be achieved. One the other hand, if more than one sequence have duty factors 1, all coded packets are in collisions so that the receiver cannot correctly receive any coded packet, even with SIC.

Below we provide a proof of the necessary statement of Theorem 4, which is divided into two main parts:

A. Proof of the necessary condition for SI property

Let R_i be the targeted information rate of user i for $i = 1, 2, \ldots, M$, such that $\sum_{i=1}^{M} R_i = 1$, i.e, the point $(R_1, R_2, \ldots, R_M)$ is on the outer boundary of $\mathcal{C}_{s0}$. The SIC procedure terminates

after some iterations if either no user's source packets can be decoded or all users' source packets have been decoded. Different users' source packets may be decoded in different SIC iterations, and moreover, the decoding order may depend on the relative shift vector $\boldsymbol{\tau}_{\mathcal{M}}$. However, it is easy to see that only the user with the duty factor 1 has source packets decoded at the first iteration for any $\boldsymbol{\tau}_{\mathcal{M}}$. We label this user as user h.

Without lost of generality, we can regard the relative shifts $\tau_1, \tau_2, \ldots, \tau_M$ as independent and identically distributed random variables that are equally likely to take on any value of $0, 1, 2, \ldots, L-1$.

Given the sequence period L, define $T_h(\boldsymbol{\tau}_{\mathcal{M}})$ as the total number of slots within an arbitrary window of L consecutive time slots on the receiver's clock that the receiver receives coded packets correctly from user h in the first SIC iteration, for the relative shift vector $\boldsymbol{\tau}_{\mathcal{M}}$. By the definition of $T_h(\boldsymbol{\tau}_{\mathcal{M}})$, for any $\boldsymbol{\tau}_{\mathcal{M}}$, it follows that:

$$T_h(\boldsymbol{\tau}_{\mathcal{M}}) = \sum_{n=0}^{L-1} s_h(n-\tau_h) \prod_{j=1, j\neq h}^{M} \big(1 - s_j(n-\tau_j)\big). \tag{3}$$

We also define $\overline{T_h}$ as the average $T_h(\boldsymbol{\tau}_{\mathcal{M}})$ computed over all possible $\boldsymbol{\tau}_{\mathcal{M}}$s.

It then follows that

$$LR_h = T_h(\boldsymbol{\tau}_{\mathcal{M}}) = \overline{T_h}, \tag{4}$$

for any $\boldsymbol{\tau}_{\mathcal{M}}$, due to the following arguments:

(i) If $LR_h > T_h(\boldsymbol{\tau}^*_{\mathcal{M}})$ for some specific choice $\boldsymbol{\tau}^*_{\mathcal{M}}$, the receiver cannot decode user h's source packets for the relative shift vector $\boldsymbol{\tau}^*_{\mathcal{M}}$.

(ii) If $LR_h < T_h(\boldsymbol{\tau}^*_{\mathcal{M}})$ for some specific choice $\boldsymbol{\tau}^*_{\mathcal{M}}$, some correctly received information is useless to decode the source packets of user h for the relative shift vector $\boldsymbol{\tau}^*_{\mathcal{M}}$. Hence, $\sum_{i=1}^{M} R_i < 1$, i.e, the point $(R_1, R_2, \ldots, R_M)$ is not on the outer boundary of $\mathcal{C}_{s0}$.

(iii) The arguments in (i),(ii) show that LR_h must be equal to $T_h(\boldsymbol{\tau}_{\mathcal{M}})$ for any $\boldsymbol{\tau}_{\mathcal{M}}$.

(iv) As R_h is a constant over the relative shift, by (iii) we obtain $T_h(\boldsymbol{\tau}_{\mathcal{M}}) = \overline{T_h}$ for any $\boldsymbol{\tau}_{\mathcal{M}}$.

From the expression in (3), one sees that $T_h(\boldsymbol{\tau}_{\mathcal{M}})$ is equal to $H(\mathbf{b}^*_{\mathcal{M}}; \boldsymbol{\tau}_{\mathcal{M}}; \mathcal{M})$ with a particular $\mathbf{b}^*_{\mathcal{M}}$ such that $b_h = 1$, $b_j = 0$ for all $j \neq h$. Furthermore, (4) shows that $H(\mathbf{b}^*_{\mathcal{M}}; \boldsymbol{\tau}_{\mathcal{M}}; \mathcal{M}) > 0$, and is SI. Therefore, by Lemma 6 we obtain that $H(\mathbf{b}_{\mathcal{A}}; \boldsymbol{\tau}_{\mathcal{A}}; \mathcal{A})$ is SI for any $\mathcal{A}$ in $\mathcal{M}$ and any $\mathbf{b}_{\mathcal{A}}$. This property implies that protocol sequences achieving zero-error capacity 1 of a CCw/oFB model with SIC must be SI.

B. Proof of the necessary condition for duty factors

As users with zero targeted information rates must have zero duty factors, we only focus on those users with positive targeted information rates. We define $\mathcal{G} := \{g_1, g_2, \ldots, g_\alpha\}$ as a collection of the indices of users who have positive targeted information rates. Obviously, $1 \le \alpha \le M$ and $\sum_{i=1}^{\alpha} R_{g_i} = 1$. In a communication session with the relative shift vector $\boldsymbol{\tau}_{\mathcal{M}}$, assume that user g_i's source packets are decoded in the π_{g_i}-th SIC iteration, for $i = 1, 2, \ldots, \alpha$.

We first aim to show $\pi_{g_i} \neq \pi_{g_j}$ for any $i \neq j$. Suppose two arbitrary users g_{i_1}, g_{i_2} simultaneously decode their source packets in a given iteration. In Section V.A, we have proved that protocol sequences achieving zero-error capacity 1 of a CCw/oFB model with SIC must be SI. By Lemma 6, we further know that $H(\mathbf{b}^*_{\mathcal{M}}; \boldsymbol{\tau}_{\mathcal{M}}; \mathcal{M})$ is SI for a particular $\mathbf{b}^*_{\mathcal{M}}$ such that $b_{g_{i_1}} = b_{g_{i_2}} = 1$, $b_{g_i} = 0$ for all $i \neq i_1, i_2$. By Lemma 1, this property implies that in an arbitrary window of L consecutive time slots, there always exists at least one slot in which only users g_{i_1}, g_{i_2} are transmitting. Obviously, these corresponding slots provide no information to the receiver, and hence the zero-error capacity 1 cannot be achieved. Therefore, the SIC iteration order must satisfy the condition: $\pi_{g_i} \neq \pi_{g_j}$ for any $i \neq j$. This implies that at an iteration one and only one user can decode its source packets.

Given a relative shift vector $\boldsymbol{\tau}_{\mathcal{M}}$, without lost of generality, for $k = 1, 2, \ldots, \alpha$, we assume an ordered tuple $(q_1, q_2, \ldots, q_\alpha)$ such that user q_k decodes its source packets at the k-th iteration. For $k = 1, 2, \ldots, \alpha$, we must have:

$$\begin{cases} LR_{q_k} \le \sum_{n=0}^{L-1} s_{q_k}(n - \tau_{q_k}) \prod_{j=k+1}^{\alpha} \big(1 - s_{q_j}(n - \tau_{q_j})\big), \\ LR_{q_i} > \sum_{n=0}^{L-1} s_{q_i}(n - \tau_{q_i}) \prod_{j=k, j\neq i}^{\alpha} \big(1 - s_{q_j}(n - \tau_{q_j})\big) \quad \text{for } k+1 \le i \le \alpha. \end{cases} \tag{5}$$

As $H(\mathbf{b}_{\mathcal{A}}; \boldsymbol{\tau}_{\mathcal{A}}; \mathcal{A})$ is SI for any $\mathcal{A}$ in $\mathcal{M}$ and any $\mathbf{b}_{\mathcal{A}}$, the right hands of both equations in (5) are independent of $\boldsymbol{\tau}_{\mathcal{M}}$. It follows that this ordered tuple $(q_1, q_2, \ldots, q_\alpha)$ can work for any $\boldsymbol{\tau}_{\mathcal{M}}$. Furthermore, we can conclude that $(q_1, q_2, \ldots, q_\alpha)$ is the unique solution to the SIC iteration order for any $\boldsymbol{\tau}_{\mathcal{M}}$, otherwise (5) cannot hold for some k when there is another solution.

By (5), Lemma 1 and the SI property, we can obtain:

$$p_{q_k} \prod_{j=k+1}^{\alpha} (1 - p_{q_j}) \ge R_{q_k}, \tag{6}$$

for $k = 1, 2, \ldots, \alpha$. Here, $\prod_{j=\alpha+1}^{\alpha} (1 - p_{q_j})$ is defined as 1, as the empty product is equal to 1

by convention. Then by recursively using (6), for $k = 1, 2, \ldots, \alpha$, we find:

$$p_{q_k} \geq \frac{R_{q_k}}{1 - \sum_{j=k+1}^{\alpha} R_{q_j}}. \tag{7}$$

Here, $\sum_{j=\alpha+1}^{\alpha} R_{q_j}$ is defined as 0, as the empty summation is equal to 0 by convention.

If $p_{q_k} > \frac{R_{q_k}}{1-\sum_{j=k+1}^{\alpha} R_{q_j}}$ for some $2 \leq k \leq \alpha$, by recursively using (6), it is easy to see

$$p_{q_1} > \frac{R_{q_1}}{1 - \sum_{j=2}^{\alpha} R_{q_j}} = 1$$

as $\sum_{j=1}^{\alpha} R_{q_j} = 1$. It is obviously impossible for a duty factor to be larger than one. Hence, we can further write (7) as

$$p_{q_k} = \frac{R_{q_k}}{1 - \sum_{j=k+1}^{\alpha} R_{q_j}}. \tag{8}$$

for $k = 1, 2, \ldots, \alpha$.

Therefore, we arrive at the conclusion that $p_{q_1} = \frac{R_{q_1}}{1-\sum_{j=2}^{M} R_{q_j}}, p_{q_2} = \frac{R_{q_2}}{1-\sum_{j=3}^{M} R_{q_j}}, \ldots, p_{q_M} = R_{q_M}$, in which $(q_1, q_2, \ldots, q_M)$ is a permutation of $(1, 2, \ldots, M)$.

C. *Sufficient conditions*

In a random access scheme without time synchronization, the receiver is required to identify the sender of each successfully received packet for any possible set of time offsets (the *identification* problem); and, to exploit SIC, the receiver is further required to find the location of each collided packet that the receiver wants to apply the interference cancellation procedure for any possible set of relative time offsets (the *location* problem).

In [1], Massey and Mathys devised a decimation algorithm to solve the identification problem for the SI sequences they constructed. They also devised an approach to solve the location problem. Shum et al. in [7] proposed a more general algorithm to solve the identification problem for all SI sequences. All these algorithms merely rely on observations of channel states, namely, whether a given past time slot contains a collision, an uncollided transmission, or no transmission at all.

In addition, [1] presented a *maximum-erasure-burst-correcting* (MEBC) coding which can encode a block of m_i Q-ry source packets to a block of n_i coded packets, with any $1 \leq m_i \leq n_i$ and any $Q \geq 2$, such that the m_i source packets can be decoded if any m_i of the n_i coded packets can be received correctly.

Based on these previously known results on identification, location and coding, we present a method to achieve zero-capacity 1 for a CCw/oFB model with SIC by using SI sequences and MEBC coding. The key idea is summarized in the following lemma.

Lemma 7. *Let* $(R_1, R_2, \ldots, R_M)$ *be an arbitrary information rate vector with nonnegative, rational components such that* $\sum_{i=1}^{M} R_i = 1$. *Let* $(q_1, q_2, \ldots, q_M)$ *be a permutation of* $(1, 2, \ldots, M)$. *A SI sequence set with duty factors* $p_{q_1} = \frac{R_{q_1}}{1-\sum_{j=2}^{M} R_{q_j}}, p_{q_2} = \frac{R_{q_2}}{1-\sum_{j=3}^{M} R_{q_j}}, \ldots, p_{q_M} = R_{q_M}$ *and period* L *can achieve the information rate* R_i *for user* i *without error for* $i = 1, 2, \ldots, M$, *by means of SIC, if user* i *for* $i = 1, 2, \ldots, M$, *employs MEBC coding to encode blocks of* $m_i = R_i L$ *source packets into blocks of* $n_i = p_i L$ *coded packets for transmission during successive slots in which user* i *actually uses the channel,*

Proof: We define an ordered tuple $(q_1, q_2, \ldots, q_M)$ such that the source packets of user q_k are decoded at the k-th iteration for $k = 1, 2, \ldots, M$. Given an arbitrary window of L consecutive time slots on the receiver's clock, for $k = 1, 2, \ldots, M$, define T_{q_k} as the number of correctly received coded packets from user q_k in the k-th iteration.

For user q_1, as no signals from any coded packets have been canceled by SIC at the beginning of the first iteration, by using the defining property of SI protocol sequences, Lemma 1 and Lemma 6, we can show that:

$$\begin{aligned}
T_{q_1} &= \frac{LH(1;\tau_{q_1};q_1)\prod_{l=2}^{M} H(0;\tau_{q_l};q_l)}{L^M} \\
&= Lp_{q_1}\prod_{l=2}^{M}(1-p_{q_l}) \\
&= \frac{LR_{q_1}}{1-\sum_{j=2}^{M} R_{q_j}}\prod_{l=2}^{M}\left(1-\frac{R_{q_l}}{1-\sum_{j=l+1}^{M} R_{q_j}}\right) \\
&= R_{q_1}L = m_{q_1}
\end{aligned}$$

for any relative shifts. Hence, the information rate R_{q_1} can be achieved for user q_1 without error. At the end of the first iteration, the interference from user q_1 in all packet transmission signals it has collision with other users can be removed by the receiver.

In the second iteration, we only need to consider the transmissions of the remaining $M-1$

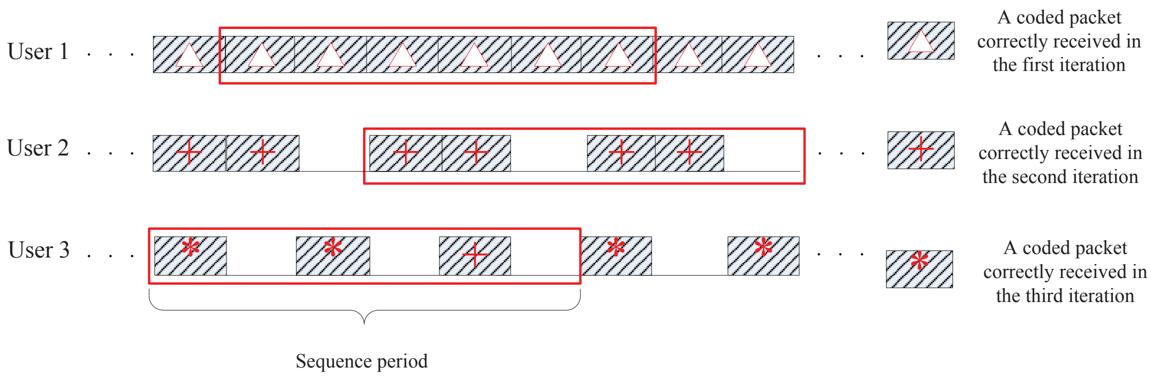

Fig. 3. An SIC procedure for protocol sequences based schemes achieving zero-error capacity 1.

users. Similarly, we find:

$$T_{q_2} = \frac{LR_{q_2}}{1-\sum_{j=3}^{M} R_{q_j}} \prod_{l=3}^{M} \Big(1 - \frac{R_{q_l}}{1-\sum_{l=j+1}^{M} R_{q_l}}\Big)$$
$$= R_{q_2}L = m_{q_2}$$

for any relative shifts. Then, the information rate R_{q_2} can also be achieved for user q_2 without error.

By repeating the above process for the remaining SIC iterations, within any arbitrary window of L consecutive time slots on the receiver's clock, we can always find the number of correctly received coded packets from user q_k in the k-th iteration is equal to m_{q_k}, for $1, 2, \ldots, M$. Hence, the corresponding zero-error information rate is R_i for each i. ■

Example: By Lemma 7, the following SI sequence set with $p_1 = 1$, $p_2 = \frac{2}{3}$, $p_3 = \frac{1}{2}$ can produce the information rate factor $(R_1 = \frac{1}{6}, R_2 = \frac{1}{3}, R_3 = \frac{1}{2})$ without error by SIC, if we set $(n_1 = 6, m_1 = 1)$, $(n_2 = 4, m_2 = 2)$ and $(n_3 = 3, m_3 = 3)$ in MEBC coding.

$$\mathbf{s}_1 = [1\ 1\ 1\ 1\ 1\ 1]$$

$$\mathbf{s}_2 = [1\ 1\ 0\ 1\ 1\ 0]$$

$$\mathbf{s}_3 = [1\ 0\ 1\ 0\ 1\ 0]$$

Fig. 3 presents an SIC procedure for this example.

In addition to the question of achieving zero-capacity 1, one may also be interested in the decoding delay of user i, that is defined as the duration (i.e., number of slots) from the

beginning of a transmission of a block of n_i coded packets sent from user i to the end of successfully decoding the corresponding m_i source packets. For the zero-capacity 1 achieving method presented in Lemma 7, as user q_1 decodes its source packets at the first iteration, it is easy to see that the decoding delay of user q_1 is at most L time slots no matter what the relative shifts are. For user q_2 that decodes its source packets at the second iteration, since that its transmission of a block of n_{q_2} coded packets may be interfered by two successive blocks of coded packets sent from user q_1 as illustrated in Fig. 3, we observe that the decoding delay of user q_2 is at most $2L$ time slots. By parity of reasoning, we can find that the decoding delay of user q_k is at most kL time slots, for $k = 3, 4, \ldots, M$.

VI. Conclusion

This paper extends the CCw/oFB model of Massey and Mathys to include SIC to iteratively resolve collisions. We have characterized the zero-error capacity region for the slot-synchronous case and presented a scheme to achieve capacity 1 rate vectors with rational components, which are shown to situate at the outer boundary of the capacity region. The scheme is based on the classical protocol sequences and erasure correcting coding approach, but requires a judicious selection of duty factors. It is interesting to note that the zero-error capacity region coincides with that of a TDMA system. Moreover, we have proved that SI sequences with some special combinations of duty factors provide the only solutions to achieve zero-error capacity 1. This implies that the minimum-period SI sequences are the shortest solutions to this problem. In particular, the minimum period in the symmetric case is $M!$.

Appendix

Obviously, (ii) $\Rightarrow$ (i). Hence, we only prove (i) $\Rightarrow$ (ii) in the following.

Divide $\mathcal{M}$ into two disjoint subsets: $\mathcal{A} = \{i_1, i_2, \ldots, i_K\}$ and $\mathcal{B} = \{i_{K+1}, i_{K+2}, \ldots, i_M\}$ for some $1 \leq K \leq M-1$. Let $\mathbf{b}^*_{\mathcal{M}} := (b^*_{i_1}, b^*_{i_2}, \ldots, b^*_{i_M})$, $\mathbf{b}^*_{\mathcal{A}} := (b^*_{i_1}, b^*_{i_2}, \ldots, b^*_{i_K})$, and $\mathbf{b}^*_{\mathcal{B}} := (b^*_{i_{K+1}}, b^*_{i_{K+2}}, \ldots, b^*_{i_M})$.

We assume that sequences with indices in $\mathcal{B}$ have the same relative shifts, by setting $\boldsymbol{\tau}^*_{\mathcal{B}} = (\varepsilon, \varepsilon, \ldots, \varepsilon)$. Also fix the values of components in $\boldsymbol{\tau}^*_{\mathcal{A}}$ by setting $\boldsymbol{\tau}^*_{\mathcal{A}} = (\tau^*_{i_1}, \ldots, \tau^*_{i_K})$. We then

have the following elementary property for generalized Hamming cross-correlation:

$$\begin{aligned}\sum_{\varepsilon=0}^{L-1} H\Big(\mathbf{b}^*_{\mathcal{M}}; (\boldsymbol{\tau}^*_{\mathcal{A}}, \boldsymbol{\tau}^*_{\mathcal{B}}); \mathcal{M}\Big) &= \sum_{\varepsilon=0}^{L-1}\sum_{n=0}^{L-1}\prod_{j=1}^{K}\delta_{s_{i_j}(n-\tau^*_{i_j})b^*_{i_j}}\prod_{j=K+1}^{M}\delta_{s_{i_j}(n-\varepsilon)b^*_{i_j}} \\ &= \sum_{n=0}^{L-1}\prod_{j=1}^{K}\delta_{s_{i_j}(n-\tau^*_{i_j})b^*_{i_j}}\sum_{\varepsilon=0}^{L-1}\prod_{j=K+1}^{M}\delta_{s_{i_j}(n-\varepsilon)b^*_{i_j}} \\ &= H\Big(\mathbf{b}^*_{\mathcal{B}}; \boldsymbol{\tau}^*_{\mathcal{B}}; \mathcal{B}\Big)\sum_{n=0}^{L-1}\prod_{j=1}^{K}\delta_{s_{i_j}(n-\tau^*_{i_j})b^*_{i_j}} \\ &= H\Big(\mathbf{b}^*_{\mathcal{B}}; \boldsymbol{\tau}^*_{\mathcal{B}}; \mathcal{B}\Big) H\Big(\mathbf{b}^*_{\mathcal{A}}; \boldsymbol{\tau}^*_{\mathcal{A}}; \mathcal{A}\Big). \end{aligned} \tag{9}$$

Keep the $\boldsymbol{\tau}^*_{\mathcal{B}}$ unchanged and change $\boldsymbol{\tau}^*_{\mathcal{A}}$ to any $\boldsymbol{\tau}^{**}_{\mathcal{A}}$. By the similar derivation of (9), we also can establish the following equality:

$$\sum_{\varepsilon=0}^{L-1} H\Big(\mathbf{b}^*_{\mathcal{M}}; (\boldsymbol{\tau}^*_{\mathcal{B}}, \boldsymbol{\tau}^{**}_{\mathcal{A}}); \mathcal{M}\Big) = H\Big(\mathbf{b}^*_{\mathcal{B}}; \boldsymbol{\tau}^*_{\mathcal{B}}; \mathcal{B}\Big) H\Big(\mathbf{b}^*_{\mathcal{A}}; \boldsymbol{\tau}^{**}_{\mathcal{A}}; \mathcal{A}\Big). \tag{10}$$

As $H(\mathbf{b}^*_{\mathcal{M}}; \boldsymbol{\tau}_{\mathcal{M}}; \mathcal{M}) > 0$ for any $\boldsymbol{\tau}_{\mathcal{M}}$, and is SI, we have

$$\sum_{\varepsilon=0}^{L-1} H\Big(\mathbf{b}^*_{\mathcal{M}}; (\boldsymbol{\tau}^*_{\mathcal{A}}, \boldsymbol{\tau}^*_{\mathcal{B}}); \mathcal{M}\Big) = \sum_{\varepsilon=0}^{L-1} H\Big(\mathbf{b}^*_{\mathcal{M}}; (\boldsymbol{\tau}^{**}_{\mathcal{A}}, \boldsymbol{\tau}^*_{\mathcal{B}}); \mathcal{M}\Big) > 0,$$

which by (9), (10) implies that

$$H\Big(\mathbf{b}^*_{\mathcal{A}}; \boldsymbol{\tau}^*_{\mathcal{A}}; \mathcal{A}\Big) = H\Big(\mathbf{b}^*_{\mathcal{A}}; \boldsymbol{\tau}^{**}_{\mathcal{A}}; \mathcal{A}\Big). \tag{11}$$

Since that the choices of $\mathcal{A}$, $\boldsymbol{\tau}^{**}_{\mathcal{A}}$ are both arbitrary in (11), we find that $H\Big(\mathbf{b}^*_{\mathcal{A}}; \boldsymbol{\tau}_{\mathcal{A}}; \mathcal{A}\Big)$ is SI for any $\mathcal{A}$ in $\mathcal{M}$.

The above conclusion is only valid for $\mathbf{b}^*_{\mathcal{A}}$. In the following, we hence are going to prove $H\Big(\mathbf{b}_{\mathcal{A}}; \boldsymbol{\tau}_{\mathcal{A}}; \mathcal{A}\Big)$ is SI for any $\mathcal{A}$ in $\mathcal{M}$ and any $\mathbf{b}_{\mathcal{A}}$ by induction on $|\mathcal{A}|$.

When $|\mathcal{A}| = 1$, $H\Big(1; \tau_{i_j}; \{i_j\}\Big) = w_{i_j}$ and is obviously SI for any $i_j \in \mathcal{M}$; and $H\Big(0; \tau_{i_j}; \{i_j\}\Big) = L - w_{i_j}$ and is obviously SI for any $i_j \in \mathcal{M}$, too.

When $|\mathcal{A}| = 2$, without loss of generalization, consider $\mathcal{A} = \{i_1, i_2\}$ in $\mathcal{M}$, $\mathbf{b}^*_{\mathcal{A}} = (b^*_{i_1}, b^*_{i_2})$. Write $\overline{b^*_{i_j}} := 1 - b^*_{i_j}$ for any i_j. By the principle of inclusion-and-exclusion, $H\Big((b^*_{i_1}, b^*_{i_2}); (\tau_{i_1}, \tau_{i_2}); \{i_1, i_2\}\Big)$ can be expressed in terms of some 1-wise or 2-wise generalized Hamming cross-correlations as

the following:

$$H\Big((b^*_{i_1}, b^*_{i_2});(\tau_{i_1}, \tau_{i_2}); \{i_1, i_2\}\Big) = H\Big(b^*_{i_1}; \tau_{i_1}; \{i_1\}\Big) - H\Big((b^*_{i_1}, \overline{b^*_{i_2}}); (\tau_{i_1}, \tau_{i_2}); \{i_1, i_2\}\Big) \tag{12}$$

$$= H\Big(b^*_{i_2}; \tau_{i_2}; \{i_2\}\Big) - H\Big((\overline{b^*_{i_1}}, b^*_{i_2}); (\tau_{i_1}, \tau_{i_2}); \{i_1, i_2\}\Big) \tag{13}$$

$$= H\Big(b^*_{i_2}; \tau_{i_2}; \{i_2\}\Big) - H\Big(\overline{b^*_{i_1}}; \tau_{i_1}; \{i_1\}\Big) + H\Big((\overline{b^*_{i_1}}, \overline{b^*_{i_2}}); (\tau_{i_1}, \tau_{i_2}); \{i_1, i_2\}\Big) \tag{14}$$

We have proved that all 1-wise generalized Hamming cross-correlations are SI, as well as $H\Big((b^*_{i_1}, b^*_{i_2}); (\tau_{i_1}, \tau_{i_2}); \{i_1, i_2\}\Big)$. Hence, $H\Big((b_{i_1}, b_{i_2}); (\tau_{i_1}, \tau_{i_2}); \{i_1, i_2\}\Big)$ must be SI for any (b_{i_1}, b_{i_2}) by the above equations (12), (13), (14). As the choice of $\mathcal{A} = \{i_1, i_2\}$ is arbitrary, we conclude that $H\Big(\mathbf{b}_{\mathcal{A}}; \boldsymbol{\tau}_{\mathcal{A}}; \mathcal{A}\Big)$ is SI for any $\mathcal{A}$ in $\mathcal{M}$ and any $\mathbf{b}_{\mathcal{A}}$, when $|\mathcal{A}| = 2$. In other words, all 2-wise generalized Hamming cross-correlations have been proved SI.

Suppose that all $(|\mathcal{A}| - 1)$-wise generalized Hamming cross-correlations are SI. Now we aim to prove this result also holds for any $|\mathcal{A}|$-wise generalized Hamming cross-correlation.

If $\mathbf{b}_{\mathcal{A}}$, $\mathbf{b}'_{\mathcal{A}}$ are only different in the j^*-th component, it is easy to see

$$H\Big(\mathbf{b}_{\mathcal{A}}; \boldsymbol{\tau}_{\mathcal{A}}; \mathcal{A}\Big) + H\Big(\mathbf{b}'_{\mathcal{A}}; \boldsymbol{\tau}_{\mathcal{A}}; \mathcal{A}\Big) = H\Big(\mathbf{b}_{\mathcal{A}\setminus\{i_{j^*}\}}; \boldsymbol{\tau}_{\mathcal{A}\setminus\{i_{j^*}\}}; \mathcal{A} \setminus \{i_{j^*}\}\Big). \tag{15}$$

By iteratively using (15), $H\Big(\mathbf{b}_{\mathcal{A}}; \boldsymbol{\tau}_{\mathcal{A}}; \mathcal{A}\Big)$ with any $\mathbf{b}_{\mathcal{A}}$ can always be written in terms of a linear combination of some $(|\mathcal{A}| - 1)$-wise generalized Hamming cross-correlations and one previously proved SI $|\mathcal{A}|$-wise generalized Hamming cross-correlation: $H\Big(\mathbf{b}^*_{\mathcal{A}}; \boldsymbol{\tau}_{\mathcal{A}}; \mathcal{A}\Big)$. Therefore, $H\Big(\mathbf{b}_{\mathcal{A}}; \boldsymbol{\tau}_{\mathcal{A}}; \mathcal{A}\Big)$ is SI for any $\mathcal{A}$ in $\mathcal{M}$ and any $\mathbf{b}_{\mathcal{A}}$, i.e., all $|\mathcal{A}|$-wise generalized Hamming cross-correlations are SI.

By induction on $|\mathcal{A}|$ starting from $|\mathcal{A}| = 2$, we can show that $H\Big(\mathbf{b}_{\mathcal{A}}; \boldsymbol{\tau}_{\mathcal{A}}; \mathcal{A}\Big)$ is SI for any $\mathcal{A}$ in $\mathcal{M}$ and any $\mathbf{b}_{\mathcal{A}}$. This completes the proof.

REFERENCES

[1] J. L. Massey and P. Mathys, "The collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 31, no. 2, pp. 192–204, Mar. 1985.

[2] E. Paolini, G. Liva, and M. Chiani, "Coded slotted ALOHA: A graph-based method for uncoordinated multiple access," *IEEE Trans. Inf. Theory*, vol. 61, no. 12, pp. 6815–6832, Dec. 2015.

[3] E. Casini, R. De Gaudenzi, and O. del Rio Herrero, "Contention resolution diversity slotted ALOHA (CRDSA): An enhanced random access scheme for satellite access packet networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 4, pp. 1408–1419, Apr. 2007.

[4] G. Liva, "Graph-based analysis and optimization of contention resolution diversity slotted ALOHA," *IEEE Trans. Commun.*, vol. 59, no. 2, pp. 477–487, Feb. 2011.

[5] C. Stefanović and P. Popovski, "ALOHA random access that operates as a rateless code," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4653–4662, Nov. 2013.

[6] R. De Gaudenzi, O. del Rio Herrero, G. Acar, and E. G. Barrabés, "Asynchronous contention resolution diversity ALOHA: Making CRDSA truly asynchronous," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6193–6206, Nov. 2014.

[7] K. W. Shum, C. S. Chen, C. W. Sung, and W. S. Wong, "Shift-invariant protocol sequences for the collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3312–3322, Jul. 2009.

[8] J. Hui, "Multiple accessing for the collision channel without feedback," *IEEE J. Select. Areas Commun.*, vol. 2, no. 4, pp. 575–582, Jul. 1984.

[9] G. Thomas, "Capacity of the wireless packet collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 1141–1144, May 2000.

[10] S. Tinguely, M. Rezaeian, and A. J. Grant, "The collision channel with recovery," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3631–3638, Oct. 2005.

[11] Y. Zhang, Y.-H. Lo, W. S. Wong, and F. Shu, "Protocol sequences for the multiple-packet reception channel without feedback," *IEEE Trans. Commun.*, vol. 64, no. 4, pp. 1687–1698, Apr. 2016.

[12] D. V. Sarwate and M. B. Pursley, "Cross-correlation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, no. 5, pp. 593–619, May 1980.